White Paper | May 2006

The New Apple of Malware's Eye: Is Mac OS X the Next Windows?

Table of Contents

Key Findings

1. From 2003 to 2005, the annual rate of vulnerability discovery on Apple's Mac OS platform has increased by 228 percent (Figure 2), compared to Microsoft's products which only saw a 73 percent increase.

2. As demonstrated by its March 2006 patch, which corrected 20 vulnerabilities, Apple's Mac OS platform is just as vulnerable to targeted malware attacks as other operating systems (Page 6).

3. Security researchers and hackers will increasingly target the Mac OS and other Apple products, such as iTunes and iPods (Page 6).

Introduction

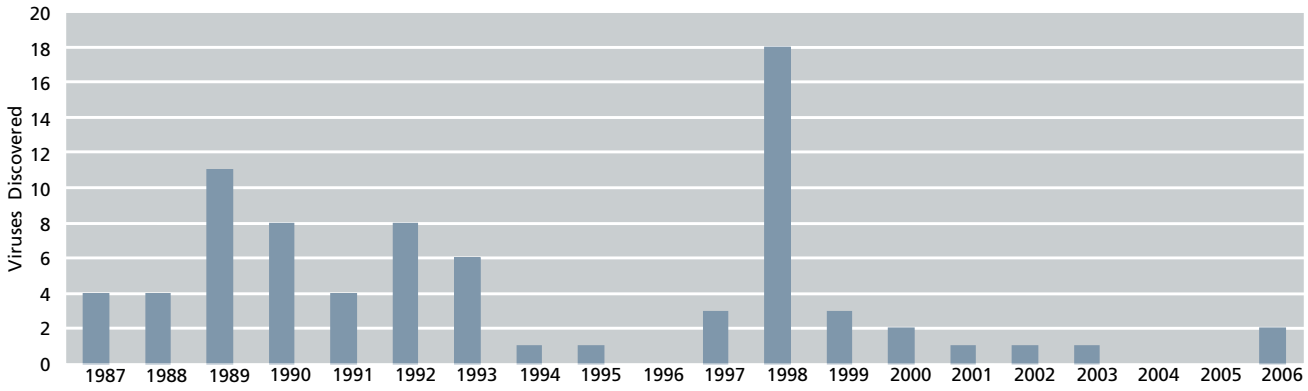
For more than 26 years, Apple Computer has, for the most part, avoided the security spotlight. This good fortune is at least partly due to its significantly smaller share of the personal computer market, especially when compared to behemoth Microsoft. In fact, Apple has been perceived as a platform and technology that is "virus free" and "immune" to security flaws – particularly those that have plagued Microsoft over the past 20 years. But as Apple's Macintosh OS X operating system (Mac OS) gains ground in the market and Apple's consumer technologies, such as iPod and iTunes, continue to enjoy widespread popularity, security researchers and hackers will increasingly point their digital lock picks toward the Mac OS and other Apple products, making Apple a growing target for malware attacks.

Apple's Increasing Exposure

Until recently, Apple's small 2.2% to 2.3% share of the global personal computer market[1] has, more than anything else, protected it from the attentions of malware authors. Since 1987 McAfee AVERT labs has documented just 76 viruses targeted at the Mac OS (see Figure 1 for the annual distribution). Compared to the 168,000 threats, including about 100,000 viruses, targeted at Windows devices from 1986 through the end of 2005, the contrast is striking.

Figure 2, however, gives Apple owners few reasons to be optimistic about the future. The National Vulnerability Database shows an increase of 228 percent in the annual vulnerability discovery rate for Apple's products from 2003 (45 vulnerabilities) to 2005 (143 vulnerabilities). In contrast, the annual discovery rate of vulnerabilities in Microsoft's products only grew 73 percent over the same period.[2] The emergence in 2006 of malware exploiting known and previously unknown (i.e. zero-day) vulnerabilities confirms Apple's new and unwanted position in the crosshairs of malware authors.

Apple appears to be in the earlier stages of malware evolution where exploits are written and spread as proofs-of-concept to demonstrate technical prowess and garner notoriety. While these elements remain in the Windows malware community, they are being overshadowed today by the more professional, profit-seeking malefactors. Apple's customer base is not yet an attractive enough target to warrant interest from this for-profit, criminal contingent. However, as Apple's continued market success places its products in the hands of more and more consumers, that status will inevitably change.

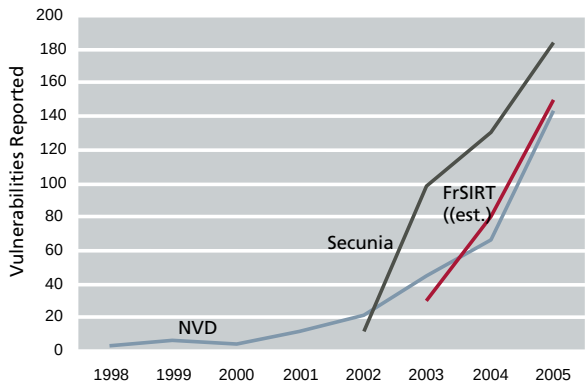


Source: McAfee AVERT Labs

Figure 1 Mac OS-targeted viruses, 1987-2006

[1] Mike Langberg: "Low Market Share is Badge of Honor, as far as Mac Faithful Are Concerned," *Mercury News*, March 26, 2006, http://www.siliconvalley.com/mld/siliconvalley/business/columnists/mike_langberg/14191452.htm?source=rss&channel=siliconvalley_mike_langberg

[2] The National Vulnerability Database reports 92 Microsoft vulnerabilities discovered in 2003 and 159 vulnerabilities in 2005, corresponding to a 73% increase.



Sources: National Vulnerability Database, French Security Incident Response Team, and Secunia

Figure 2: Apple's vulnerabilities, 1997-2006[3]

OSX/Leap: A Leap into the Unknown for Macintosh

Designed to propagate via the AIM/iChat instant messaging system, *OSX/Leap*[4] is the first virus to attack the Mac OS X platform. Because the virus relies on Apple's Spotlight technology, only systems running Mac OS X version10.4 through 10.4.4 are affected. After some confidential distributions, the virus was first seen posted to the *MacRumors*[5] forum on February 13, 2006. *OSX/Leap* tricked users into downloading it by claiming to be a set of screenshots from Mac OS X 10.5 (Leopard), a version of Mac OS X under development.

Distributed as an attachment with a file size of 40,893 bytes, *OSX/Leap* allows the recipient to choose whether or not to accept the file. Once accepted, the file is saved as *latestpics.tgz* (See Figure 3).

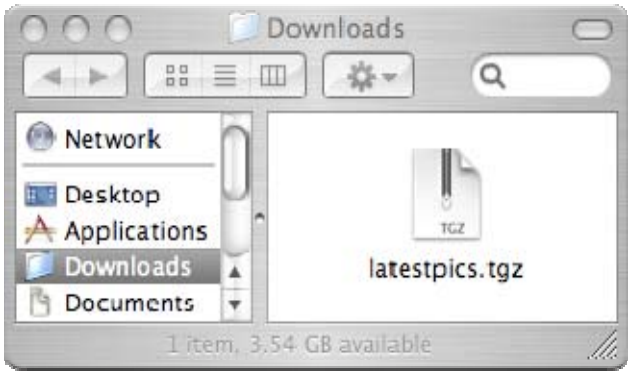


Figure 3: OSX/Leap archive after initial download.

The *.tgz* extension indicates that it is a compressed file (gzip-compressed tar file). Once decompressed, two standard Apple hierarchical file system (HFS) files appear in the folder with the filenames *._latestpics* (43,694 bytes) and ***latestpics*** (39,596 bytes).

The file *._latestpics* appears as a JPEG image icon, as seen in Figure 4, but is, in fact, an executable compiled for the PowerPC. To view the image, users are easily tempted to double-click and take a look. Once executed, the virus displays a message and copies itself to the temporary folder (/tmp) by manipulating the file (*resource fork*), using executable code contained in the *latestpics* file (*data fork*).

Figure 4: .latestpics appears as a JPEG image icon

The file replicates itself as a compressed image that it sends out in subsequent messages. It then creates its own system entry, dropping itself into either the root InputManagers directory (/Library/InputManagers/), if permissions allow, or the current user's home directory (/Users/[current user]/Library/InputManagers/). Being in the InputManagers directory causes the operating system to execute the virus whenever another application is launched. The user may be asked to enter the administrator's password to complete this process, as the virus must be able to write other files to the Applications directory (/Applications).

When executed, the virus uses the Mac's *Spotlight* search tool to identify the four most recently used applications that do not depend on administrator's rights (*root*). Once these applications are found, the virus modifies their launch processes so that it is executed first. The virus also positions markers, called *oompa* and *loompa*,[6] in the files that it has infected to avoid reinfecting them. Once the application is executed and the virus is in place, the user is notified by a "*Welcome to Darwin!*" message, see Figure 5.

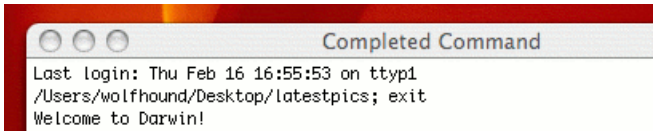


Figure 5: "Welcome to Darwin!" dialog box confirms that .latestpics virus has been executed

A bug in this process causes the infected applications to no longer run correctly. While the author appears to have planned to propagate the virus via e-mail (*mail.app)*, it actually only propagates via the instant messaging system,

[3] National Vulnerability Database: http://nvd.nist.gov/statistics.cfm, French Security Incident Response: http://www.frsirt.com/search.php, Secunia: http://secunia.com/vendor/

[4] http://vil.nai.com/vil/content/v_138578.htm

[5] http://forums.macrumors.com/

[6] The malware author apparently named the markers after the pint-sized chocolate factory workers, Oompa and Loompa, in the book Charlie and the Chocolate Factory.

sending itself to everyone on the user's buddy list (*AIM/iChat buddy list)* each time the application is launched. Thus, the virus' code has not been optimized for release in the wild and may have been programmed for test purposes only.

In a strong reaction to the OSX/Leap announcement, Apple sought to distinguish it from viruses, stating, "[OSX/Leap] is not a virus, it is malicious software that requires a user to download the application and execute the resulting file. Apple always advises Macintosh users to only accept files from vendors and Web sites that they know and trust."[7]

Though Apple correctly states that the targeted user must carry out specific actions to enable the malware's self-replicating function, its position is reminiscent of Microsoft's early reaction in 1995 to the first macro virus, *WM/Concept*, calling it a "prank macro" rather than a virus. In fact, many Windows viruses also require the user to voluntarily decompress an attachment and double-click to start an executable. Thus, by this standard, *OSX/Leap* is a virus.

The virus can be removed by first deleting the file, *latestpics,* which contains the virus itself. If the file has not been executed, removal is complete. If it has been executed, any files found in the temporary directory will need to be deleted, as well as the file */Users/[CURRENT USER*[8]*]/Library/InputManagers/apphook.bundle*. Finally, restart the machine and the virus will be completely removed. Any infected applications should also be reinstalled from backups.

OS X: The Alerts Continue . . .

Just two days after the announcement of *OSX/Leap, OSX/Inqtana.a*[9] and its variants appeared. Arriving second on the scene meant the authors probably did not get the publicity they were seeking. Unlike *OSX/Leap*, *OSX/Inqtana.a* actually exploited an OS X vulnerability in the *Bluetooth* directory traversal and file exchange services, reference number CVE-2005-1333.[10] The virus installs itself in a normally prohibited area, enabling it to execute on the next reboot. Once executed, the virus looks for *Bluetooth* devices that accept file transfers via the OBEX (OBject EXchange) service (*push* requests). If the user accepts the request on the target machine, the virus exploits the vulnerability and copies itself outside the exchange directory. Apple has a patch available on its web site for the vulnerability exploited by *OSX/Inqtana.a.*[11]

February 2006 brought two new Mac vulnerabilities into the spotlight, *OSX/Exploit-ZipShell*[12] and *OSX/Exploit-ScriptEx.*[13] The first affects *Safari* web browsers, and the second affects the *Apple Mail* e-mail application. Because both of these applications can run certain scripts with advanced permissions, they can be hijacked to run a shell script without informing the user. Intended for opening multimedia files, disk images, and archives, this vulnerability affects ZIP archives with *Safari* and AppleDouble MIME formatted files with *Apple Mail.* A hacker can exploit these vulnerabilities to run any application and potentially even take control of a machine remotely.

Fortunately, the *Thunderbird* mail client, available from the Mozilla Foundation, is unaffected by these vulnerabilities entirely because it does not honor AppleDouble/AppleFile MIME extensions. Apple has recently distributed patches[14] that correct these vulnerabilities, but users must be sure that the function "Open 'safe' files after downloading" is disabled in their web browser.

OS X: The Future

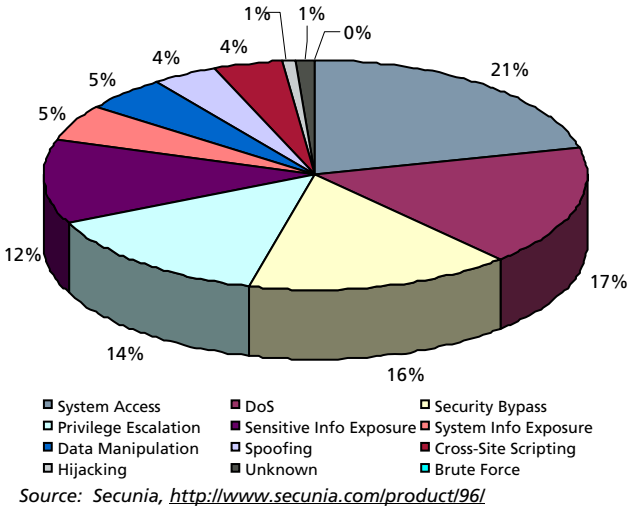
None of the recently released attacks appears to have propagated widely, perhaps due to bugs in the code and the still small marketshare of the Mac OS platform. However, with the easy availability of malware source code on the Internet, more attacks will almost certainly be launched. While the total number of OS X-targeted viruses has been relatively low since January 2004, the growing numbers of Macintosh vulnerabilities may attract more talented hackers. In fact, on February 21, 2006, the world saw its first zero-day[15] Mac-targeted attack, with the release of exploits that utilized the previously unknown vulnerabilities: *OSX/Exploit-ZipShell* and *OSX/Exploit-ScriptEx.* Apple released a security patch for the vulnerabilities 8 days later on March 1, 2006.[14]

Although many Macintosh users think their systems are safe from attack, they will have to rethink their "safe harbor" logic. In addition, Apple's recent shift to using Intel microprocessors in all new Macintoshes could usher a whole new era for Macintosh malware. Chip-level threats have not yet been seen, however, the common architecture will not go unnoticed by the malware community. In addition, virtualization technologies, such as Q, QEMU, WinTel 2.1, and Parallels Workstation – and the new Boot Camp technology from Apple give Mac users viable options for high performance computing with both the Windows and Mac OS X operating systems, making them vulnerable to threats on both platforms.

When Apple corrected the *OSX/Inqtana.a* virus vulnerability in March 2006, the same patch fixed twenty

[7] Peter Cohen, "Reports Emerge of Mac OS X Trojan Horse or Worm", *Macworld*, February 16, 2006, http://www.macworld.com/news/2006/02/16/oompa/index.php
[8] [CURRENT USER] is the name of the user session at the time the machine is infected.
[9] http://vil.nai.com/vil/content/v_138608.htm
[10] Directory traversal vulnerability in the Bluetooth file and object exchange services in Mac OS X 10.3.9 allows remote attackers to read arbitrary files: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1333
[11] Security Update 2005-005 (Client): http://www.apple.com/support/downloads/securityupdate2005005client.html
Security Update 2005-005 (Server): http://www.apple.com/support/downloads/securityupdate2005005server.html
[12] http://vil.nai.com/vil/content/v_138661.htm
[13] http://vil.nai.com/vil/content/v_138663.htm
[14] Security Update 2006-001: http://docs.info.apple.com/article.html?artnum=303382
[15] A zero-day exploit is one that utilizes a vulnerability which has not yet been corrected, i.e. no corrective patch is available.

other vulnerabilities,[16] all of which could have been exploited by local or remote attackers to escalate privileges, hijack a computer or cause a denial of service. Apple's most recently published patches correct more than fifteen additional vulnerabilities. Clearly, the Mac OS X is far from invulnerable, and Mac users, like their Windows counterparts, must remain vigilant against new and evolving threats.

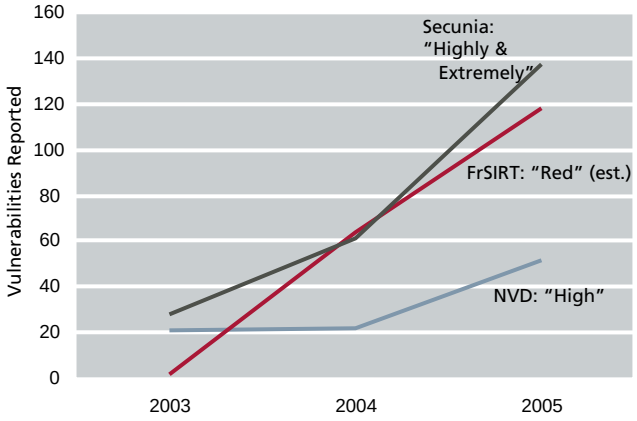


Source: Secunia, http://www.secunia.com/product/96/

Figure 6: Mac OS X attack impacts breakdown, 2003-2006

Figure 6 shows the impacts of attacks on OS X, as reported by Secunia. In Figure 7, the annual distribution of critical security vulnerabilities found in the Mac OS X platform is given from 2003 to 2005. The rapid rise reported by NIST and FrSIRT demonstrate an abiding and growing malware interest in the Mac OS X platform.[17,18]

On April 19, 2006, another six zero-day vulnerabilities were disclosed by a security researcher. These previously unknown vulnerabilities can allow a malefactor to crash or hijack a computer. Though they all require some kind of user interaction, such as opening a zip file or viewing a web page with graphics, these vulnerabilities are considered very dangerous and rated "Highly Critical."[19]



Sources: National Vulnerability Database, French Security Incident Response Team, and Secunia

Figure 7: Mac OS X vulnerabilities, 2003-2005

While the Mac's relatively small installed base has helped to limit the interest of malware authors in the platform to date, that protection is diminishing. The rising popularity of Apple's consumer products, notably the iPod media devices and iTunes media services, has helped thrust Apple into the spotlight of the malware community and has created new targets for malicious activity. In 2005, four vulnerabilities were discovered in iTunes that could be used to escalate privileges and execute arbitrary code,[20] and in February, 2006, *Slurp* became the first iPod-transported malware. *Slurp* is designed to steal business-critical information by looking through a computer's data files when an infected iPod is attached.[21]

The recent bias of malware authors toward smaller, focused attacks intent upon under-the-radar, targeted financial gains, coupled with the easy availability of Mac exploit code on the Internet, may one day make the Mac OS a tempting target for the same types of malware currently plaguing the Windows world, such as botnets, spyware, adware, SPAM, and DDOS attacks. The trend toward greater numbers of vulnerabilities and attacks against the Mac OS is evident, and Mac users would do well to take notice and become more vigilant.

[16] http://www.frsirt.com/bulletins/1155
[17] http://www.frsirt.com/searchengine.php
[18] http://secunia.com/vendor/17/
[19] http://secunia.com/advisories/19686/

[20] National Vulnerability Database: http://nvd.nist.gov/
[21] http://vil.nai.com/vil/content/v_138662.htm